


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

identifier based encryption trusted authority


 Searching within The ACM Digital Library for: identifier based encryption trusted authority (start
 Found 238 of 239,255

REFINE YOUR SEARCH

 ▼ Refine by Keywords
 identifier based encryption
 Discovered Terms

 ▼ Refine by People
[Names](#)
[Institutions](#)
[Authors](#)
[Reviewers](#)

 ▼ Refine by
[Publications](#)
[Publication Year](#)
[Publication Names](#)
[ACM Publications](#)
[All Publications](#)
[Content Formats](#)
[Publishers](#)

 ▼ Refine by
[Conferences](#)
[Sponsors](#)
[Events](#)
[Proceeding Series](#)

ADVANCED SEARCH

[Advanced Search](#)

FEEDBACK

[Please provide us with feedback](#)

Found 238 of 239,255

[Search Results](#)
[Related Journals](#)
[Related Magazines](#)
[Related SI](#)
[Related Conferences](#)

Results 1 - 20 of 238

Sort by relevance

☐ in

[Save results to a Binder](#)

Result page: 1 2 3 4 5 6 7 8 9

- 1 [Fully self-organized peer-to-peer key management for mobile ad hoc](#)
[Johann van der Merwe, Dawoud Dawoud, Stephen McDonald](#)
 September 2005 WiSe '05: Proceedings of the 4th ACM workshop on Wirele
 Publisher: ACM

 Full text available: [Pdf](#) (237.33 KB) Additional Information: [full citation](#), [abstract](#), [referer review](#)

Bibliometrics: Downloads (6 Weeks): 33, Downloads (12 Months): 140, Citatio

Mobile ad hoc networks (MANETs) offer communication over a shared w
 without any pre-existing infrastructure. Forming peer-to-peer security a
 MANETs is more challenging than in conventional networks due to the la

Keywords: Mobile IPv6, crypto-based identifiers, identity-based crypto
 hoc networks, network level key distribution, network security, pairwise
 management, peer-to-peer key management, self-organization, subordi

- 2 [The HP time vault service: exploiting IBE for timed release of confide](#)
[Marco Casassa Mont, Keith Harrison, Martin Sadler](#)
 May 2003 WWW '03: Proceedings of the 12th international conference on
 Publisher: ACM

 Full text available: [Pdf](#) (860.87 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 48, Citation (

Digital information is increasingly more and more important to enable ir
 transactions on the Internet. On the other hand, leakages of sensitive ir
 have harmful effects for people, enterprises and governments.This page

Keywords: disclosure policies, identifier-based encryption, privacy, sec
 release, web service

- 3 [What can identity-based cryptography offer to web services?](#)
[Jason Crampton, Hoon Wei Lim, Kenneth G. Paterson](#)
 November 2007 SWS '07: Proceedings of the 2007 ACM workshop on Secur
 Publisher: ACM


 Full text available: [Pdf](#) (245.87 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 40, Downloads (12 Months): 397, Citatio

Web services are seen as the enabler of service-oriented computing, a next generation distributed computing technology. Independently, identity-based cryptography is emerging as a serious contender to more conventional (public ...

Keywords: identity-based cryptography, message-level security, web s

4 [A survey on peer-to-peer key management for mobile ad hoc networks](#)

 [Johann Van Der Merwe](#), [Dawoud Dawoud](#), [Stephen McDonald](#)

April 2007 Computing Surveys (CSUR) , Volume 39 Issue 1

Publisher: ACM


Full text available:  Pdf (872.71 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 180, Downloads (12 Months): 1441, Cita

The article reviews the most popular peer-to-peer key management protocols for mobile ad hoc networks (MANETs). The protocols are subdivided into groups based on design strategy or main characteristic. The article discusses and provides


Keywords: Mobile ad hoc networks, pairwise key management, peer-to-peer key management, security

5 [Secure attribute-based systems](#)

 [Matthew Pirretti](#), [Patrick Traynor](#), [Patrick McDaniel](#), [Brent Waters](#)

October 2006 CCS '06: Proceedings of the 13th ACM conference on Computer and communications security

Publisher: ACM


Full text available:  Pdf (1.13 MB) Additional Information: [full citation](#), [abstract](#), [referer](#), [terms](#)

Bibliometrics: Downloads (6 Weeks): 37, Downloads (12 Months): 206, Citatio

Attributes define, classify, or annotate the datum to which they are associated. Traditional attribute architectures and cryptosystems are ill-equipped to handle them in the face of diverse access requirements and environments. In this pa

Keywords: applied cryptography, attribute-based encryption, secure sy

6 [Access control in publish/subscribe systems](#)

 [Jean Bacon](#), [David M. Eysers](#), [Jatinder Singh](#), [Peter R. Pietzuch](#)

July 2008 DEBS '08: Proceedings of the second international conference on Distributed event-based systems

Publisher: ACM


Full text available:  Pdf (1.30 MB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 63, Downloads (12 Months): 213, Citatio

Two convincing paradigms have emerged for achieving scalability in wide-area distributed systems: *publish/subscribe communication* and *role-based*, policy-driven access to the system by applications. A strength of publish/subscribe ...

Keywords: encryption, publish/subscribe, role based access control

7 [Beyond secure channels](#)

 [Yacine Gasmi, Ahmad-Reza Sadeghi, Patrick Stewin, Martin Unger, N. Asok](#)
November 2007 STC '07: Proceedings of the 2007 ACM workshop on Scalab
computing

Publisher: ACM


Full text available:  [Pdf](#) (963.87 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 34, Downloads (12 Months): 276, Citatio


A Trusted Channel is a secure communication channel which is cryptogr
the state of the hardware and software configurations of the endpoints.
describe secure and flexible mechanisms to establish and maintain Trus

Keywords: TLS, hypervisor, microkernel, relay attack, remote attestati
changes, trusted channel, trusted computing, virtualization

8 [Untraceable RFID tags via insubvertible encryption](#)

 [Giuseppe Ateniese, Jan Camenisch, Breno de Medeiros](#)
November 2005 CCS '05: Proceedings of the 12th ACM conference on Comp
communications security

Publisher: ACM


Full text available:  [Pdf](#) (238.38 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)
[terms](#)

Bibliometrics: Downloads (6 Weeks): 34, Downloads (12 Months): 248, Citatio

We introduce a new cryptographic primitive, called *insubvertible encryp*
produces ciphertexts which can be randomized without the need of any
Unlike plain universal re-encryption schemes, insubvertible encryption p

Keywords: RFID privacy, bilinear maps, universal re-encryption

9 [Black-box accountable authority identity-based encryption](#)

 [Vipul Goyal, Steve Lu, Amit Sahai, Brent Waters](#)
October 2008 CCS '08: Proceedings of the 15th ACM conference on Comput
communications security

Publisher: ACM

Full text available:  [Pdf](#) (283.31 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 62, Downloads (12 Months): 62, Citation

A well-known concern in the setting of identity based encryption is that
powerful and has to be completely trusted. To mitigate this problem, th
Accountable Authority Identity-Based Encryption (A-IBE) was recently ir

Keywords: accountable authority, identity-based encryption

10 [A secure privacy-preserving roaming protocol based on hierarchical encryption for mobile networks](#)

[Zhiguo Wan, Kui Ren, Bart Preneel](#)

March 2008 WiSec '08: Proceedings of the first ACM conference on Wireless security

Publisher: ACM


Full text available:  Pdf (241.81 KB) Additional Information: [full citation](#), [abstract](#), [referrer](#)

Bibliometrics: Downloads (6 Weeks): 28, Downloads (12 Months): 201, Citation

Roaming services in wireless networks provide people with preferable flexibility and convenience. However, such advantages should be offered with both security and privacy in mind. With consideration on privacy protection during roaming in wireless networks,

Keywords: mobile networks, privacy, roaming protocols

11 [Trust management for secure information flows](#)

 [Mudhakar Srivatsa, Shane Balfe, Kenneth G. Paterson, Pankaj Rohatgi](#)

October 2008 CCS '08: Proceedings of the 15th ACM conference on Computer and communications security

Publisher: ACM


Full text available:  Pdf (1.03 MB) Additional Information: [full citation](#), [abstract](#), [referrer](#)

Bibliometrics: Downloads (6 Weeks): 112, Downloads (12 Months): 112, Citation

In both the commercial and defence sectors a compelling need is emerging for a yet secure, dissemination of information across traditional organisations. In this paper we present a novel trust management paradigm for securing information flow in organisational ...

Keywords: ID-PKC, information flow, risk, trust

12 [Preventing information leakage between collaborating organisations](#)

 [Muntaha Alawneh, Imad M. Abbadi](#)

August 2008 I CEC '08: Proceedings of the 10th international conference on Information and e-commerce

Publisher: ACM


Full text available:  Pdf (658.13 KB) Additional Information: [full citation](#), [abstract](#), [referrer](#)

Bibliometrics: Downloads (6 Weeks): 25, Downloads (12 Months): 48, Citation

Information sharing and protection against leakage is a critical problem for organisations having sensitive information. Sharing content between organisations in the same organisation extends to exchanging and sharing content between organisations.


Keywords: collaborating organisations, enterprise rights management, information sharing

13 [Access control to people location information](#)

 [Urs Hengartner, Peter Steenkiste](#)

November 2005 Transactions on Information and System Security (TISSEC) Issue 4

Publisher: ACM


Full text available:  Pdf (356.85 KB) Additional Information: [full citation](#), [abstract](#), [referrer](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 35, Downloads (12 Months): 253, Citatio

Ubiquitous computing uses a variety of information for which access ne
controlled. For instance, a person's current location is a sensitive piece
that only authorized entities should be able to learn. Several challenges

Keywords: Certificates, DSA, RSA, SPKI/SDSI, credential discovery, de
location, privacy, trust

14 [Towards a secure and interoperable DRM architecture](#)

 [Gelareh Taban, Alvaro A. Cárdenas, Virgil D. Gilgor](#)

October 2006 DRM '06: Proceedings of the ACM workshop on Digital rights
Publisher: ACM


Full text available:  Pdf (442.79 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 58, Downloads (12 Months): 278, Citatio

In this paper we look at the problem of interoperability of digital rights
(DRM) systems in home networks. We introduce an intermediate module
Domain Interoperability Manager (DIM) to efficiently deal with the probl

Keywords: DRM, home networks, interoperability

15 [Authentication protocols for ad hoc networks: taxonomy and research](#)

 [Nidal Aboudagga, Mohamed Tamer Refael, Mohamed Elloweissy, Luiz A. De
Jacques Quisquater](#)

October 2005 Q2SWinet '05: Proceedings of the 1st ACM international wor
of service & security in wireless and mobile networks

Publisher: ACM


Full text available:  Pdf (314.61 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 43, Downloads (12 Months): 243, Citatio

Ad hoc networks, such as sensor and mobile ad hoc networks, must ove
of security challenges to realize their potential in both civil and military
Typically, ad hoc networks are deployed in un-trusted environments. Co


Keywords: ad hoc networks, authentication, credentials, identity verifi
security, protocol taxonomy

16 [A secure and private system for subscription-based remote services](#)

 [Pino Persiano, Ivan Visconti](#)

November 2003 Transactions on Information and System Security (TI
Issue 4

Publisher: ACM

Full text available:  Pdf (241.65 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)
[terms](#)

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 101, Citatio

In this paper we study privacy issues regarding the use of the SSL/TLS

X.509 certificates. Our main attention is placed on subscription-based re (e.g., subscription to newspapers and databases) where the service ma

Keywords: Access control, anonymity, cryptographic algorithms and pr world-wide web

17 [Digital rights management in a 3G mobile phone and beyond](#)



Thomas S. Messerges, Ezzat A. Dabbish

October 2003 DRM '03: Proceedings of the 3rd ACM workshop on Digital rig
Publisher: ACM

Full text available: Pdf (306.59 KB) Additional Information: [full citation](#), [abstract](#), [referer terms](#)

Bibliometrics: Downloads (6 Weeks): 62, Downloads (12 Months): 304, Citatio

In this paper we examine how copyright protection of digital items can l managed in a 3G mobile phone and other devices. First, the basic conce and requirements for digital rights management are reviewed. Next, a f

Keywords: MPEG-21, copyright protection, cryptography, digital conten management, embedded system, key management, mobile phone, ope security

18 [Rethinking accountable privacy supporting services: extended abstr](#)



Jan Camenisch, Thomas Groß, Thomas S. Heydt-Benjamin

October 2008 DIM '08: Proceedings of the 4th ACM workshop on Digital ide management
Publisher: ACM

Full text available: Pdf (401.09 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 20, Downloads (12 Months): 20, Citation

As privacy concerns among consumers rise, service providers will increa provide services that support privacy enhancing technologies. At the sai providers of commercial services require the security of identifying mist

Keywords: accountability, anonymous credential systems, cryptograph privacy, time capsule, verifiable encryption

19 [Security analysis of Internet technology components enabling global workplaces—a framework](#)



Manish Gupta, Shamik Banerjee, Manish Agrawal, H. Raghav Rao

September 2008 Transactions on Internet Technology (TOIT) , Volume 8
Publisher: ACM

Full text available: Pdf (1.60 MB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 199, Downloads (12 Months): 283, Citati

As organizations increasingly operate, compete, and cooperate in a glob business processes are also becoming global to propagate the benefits f and standardization across geographical boundaries. In this context, se

Keywords: Internet applications, Security analysis, globally distributed management

20 [Authorised domain management using location based services](#)



Imad Abbadi

September 2007 Mobility '07: Proceedings of the 4th international conference on technology, applications, and systems and the 1st international conference on Computer human interaction in mobile technology

Publisher: ACM

Full text available: [Pdf](#) (406.94 KB) Additional Information: [full citation](#), [abstract](#), [referer](#)

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 49, Citation

This paper focuses on creating a secure domain consisting of all devices single owner. This domain allows secure content sharing between devices and prevents the illegal copying of content to devices outside the domain.

Keywords: DRM, access control, authorised domain, copyright protection services, trusted computing

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)